INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-55512	App: 09/637,229
	Applicant: Çetin K. Koç et al.	
	Filed: August 11, 2000	Art Unit: 2766

OTHER DOCUMENTS

✓			Kaliski, Jr., B.S., "The Montgomery Inverse and Its Applications," IEEE Trans. on Computers 44:1064-1065 (August 1995)
✓			Montgomery, P.L., "Modular Multiplication Without Trial Division," Math. of Computation 44:519-521 (April 1985)
✓			Koç, Ç.K. et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," IEEE Micro 16:26-33 (June 1996)
✓			Dhem, J. et al., "SCALPS: Smart Card For Limited Payment Systems," IEEE Micro 16:42-51 (June 1996)
✓			Diffie, W., Hellman, M.E., "New Directions in Cryptography," IEEE Trans. on Information Theory 22:644-654 (1976)
✓			Rivest, R.L. et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21:120-126 (1978)
✓			Koç, Ç.K., Acar, T., "Fast Software Exponentiation in GF(2^k)" in Proceedings, 13th Symposium on Computer Arithmetic, pp. 225-231 (July 1997) (T. Lang et al., editors)
✓			Hamano, T. et al., "$O(n)$-Depth Circuit Algorithm for Modular Exponentiation" in Proceedings, 12th Symposium on Computer Arithmetic, pp. 188-192 (July 1995) (S. Knowles, W.H. McAllister, editors)
✓			Orup, H., "Simplifying Quotient Determination in High-radix Modular Multiplication" in Proceedings, 12th Symposium on Computer Arithmetic, pp. 193-199 (July 1995) S. Knowles, W.H. McAllister, editors)

EXAMINER: Michael Cheng	DATE 2-26-04

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-55512	App: 09/637,229
	Applicant: Çetin K. Koç et al.	
	Filed: August 11, 2000	Art Unit: 2766

OTHER DOCUMENTS

MV			Bernal, A., Guyot, A., "Design of a Modular Multiplier Based on Montgomery's Algorithm" in 13th Conference on Design of Circuits and Integrated Systems, pp. 680-685 (November 1998)
MV			Eldridge, S.E., Walter, C.D., "Hardware Implementation of Montgomery's Modular Multiplication Algorithm," IEEE Trans. Computers 42:693-699 (June 1993)
MV			Kornerup, P., "High-Radix Modular Multiplication for Cryptosystems" in Proceedings, 11th Symposium on Computer Arithmetic, pp. 277-283 (June 1993) (E. Swartzlander et al., editors)
MV			Walter, C.D., "Space/Time Trade-offs for Higher Radix Modular Multiplication Using Repeated Addition," IEEE Trans. Computers 46:139-141 (1997)
MV			Royo, A., et al., "Design and Implementation of a Coprocessor for Cryptography Applications," European Design and Test Conference, pp. 213-217 (March 1997)
MV			Koç, Ç.K., Acar, T., "Montgomery Multiplication in GF(2*k*), "Designs, Codes and Cryptography 14:57-69 (1998)
MV			Tenca, A.F., "Variable Long-Precision Arithmetic (VLPA) for Reconfigurable Coprocessor Architectures," Ph.D. Thesis, University of California at Los Angeles (March 1998)
MV			
MV			

EXAMINER: Michael Vaughn	DATE 2-26-04

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.

MJ:mgs 06/25/2002 245-55512 124269

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-55512	App: 09/637,229
	Applicant: Koc et al.	
	Filed: August 11, 2000	Art Unit:

U.S. PATENT DOCUMENTS

Init.*		Number	Date	Name	Class	Sub	Filed
mv		6,151,393	11/21/00	Jeong			
mv		5,742,530	4/21/98	Gressel et al.			
mv		6,049,815	4/11/00	Lambert et al.			
mv		6,035,317	3/7/00	Guy			
mv		5,867,412	2/2/99	Suh			
mv		6,209,016 B1	3/27/01	Hobson et al.			
mv		5,745,398	4/28/98	Monier			
mv		5,144,574	9/1/92	Morita			
mv		5,513,133	4/30/96	Cressel et al.			
mv		6,185,596 B1	2/6/01	Hadad et al.			
mv		5,349,551	9/20/94	Petro			
mv		6,182,104 B1	1/30/01	Foster et al.			
mv		5,954,788	9/21/99	Suh et al.			

OTHER DOCUMENTS

mv			Hong et al., "New Modular Multiplication Algorithms for Fast Modular Exponentiation," EUROCRYPT '96 Proceedings, 166-177

MJ:mgs 06/25/2002 245-55512 124269

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-55512	App: 09/637,229
	Applicant: Koc et al.	
	Filed: August 11, 2000	Art Unit:

MW			Walter, C., "Faster Modular Multiplication by Operand Scaling," Advances in Cyrptology Proc., Crypto '91, LNCS 576, 313-323 (1992)
MW			Even, S., "Systolic Modular Multiplication," Crypto 90 Proc. Lecture Notes in Computer Science no. 537, 619-624
MW			Bosselaers et al., "Comparison of Three Modular Reduction Functions," Crypto '94, 175.186

EXAMINER: Michael Chin	DATE 2-26-04

*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.